REMARKS

Applicant respectfully requests reconsideration of the present application in view of the reasons that follow.

No claims are being amended. Claims 1-20 remain pending in this application.

Rejection under 35 U.S.C. § 102

Claims 1-20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,867,578 to Brickell et al. (hereafter "Brickell"). Applicant respectfully traverses this rejection for at least the following reasons.

All of the independent claims, which are directed to a signature calculation system by use of a mobile agent, or a corresponding computer-readable record medium, contain specifically recited features which are not disclosed or suggested by Brickell. For example, each of the remote hosts in the network of claim 1 includes a partial signature calculation means, the specifically recited features of which are not disclosed or suggested by Brickell. As noted in the amendment filed on July 18, 2005, the partial signature calculation means calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent based on data input to the partial signature calculation means, namely (1) signature target data, where the signature target data is target data to which a digital signature of the owner is to be attached, (2) data which have been carried by the mobile agent including partial signature auxiliary data, where the partial signature auxiliary data is generated in the base host based in part on a secret key of the mobile agent owner, and (3) a secret key of the remote host. Brickell fails to disclose a partial signature calculation means with the features as recited in claim 1, namely a partial signature calculation means that calculates a partial signature in a remote host based on input data, where the input data falls into either category (1) or (2) above.

As pointed out in the Amendment filed on July 18, 2005, while Brickell discloses computing a signature (t,s) which is based on a number of individual values r_i and s_i calculated by the individual RCA members based on individual keys of the RCA members, Brickell does not disclose a system including a base host and remote hosts, where the partial

signatures are computed based on data input into the RCA members where that data falls into either category 1) signature target data, where the signature target data is target data to which a digital signature of the owner is to be attached, or 2) data which have been carried by a mobile agent including partial signature auxiliary data, where the partial signature auxiliary data is generated in the base host based in part on a secret key of the mobile agent owner. The individual values r_i and s_i are not calculated based on data falling into categories 1) or 2). Thus, the Brickell system is very different from that as specifically recited in claim 1.

The Office Action continues to assert that applicant has failed to explicitly identify specific claim limitations which would define a patentable distinction over the prior art. To the contrary, applicant has specifically identified features of the partial signature calculation means as recited in claim 1, which are not disclosed or suggested by Brickell. By contrast, the Office Action merely cites to Brickell at col. 7, line 36 to col. 9, line 9 as allegedly disclosing the limitations of the remote host in the claims (which includes the partial signature calculation means) without specifically pointing out in Brickell any of the specific features as recited. If the present rejection based on Brickell is maintained, the Examiner is again respectfully requested to specifically point out by specific column and line number where Brickell specifically discloses the limitations of the partial signature calculation means in the next Office Action.

Moreover, the structure of the system as recited in claim 1 provides advantages in reducing the amount of stored secret information which need be retained in each remote host as the number of mobile agents is increased, a feature which is not realized in the Brickell system. In the system of claim 1, because partial information of a secret key is not stored in a remote host, but is instead carried by a mobile agent in encrypted form, the remote host need only store a fixed amount of secret information, which is independent of the number of entities, such as mobile agents, to compute signatures. This advantage is not suggested by Brickell. The purpose of the Brickell system is to allow for the change of values of key fragments and the number of RCAs for a distributed RCA system, while the public key maintains its original value. Brickell is not per se concerned with computing the signatures of a number of different entities. In a Brickell type system, the amount of secret information

(fragments of a signature key) that must be stored by an RCA is proportional to the number of entities, such as a mobile agent, for which the RCA computes a signature.

As an example comparison between the Brickell system and that as claimed, take the situation where the system computes the signatures of 10,000 mobile agents, the system comprises 10 remote hosts, and five of the remote hosts in collaboration generate a signature. Further assume that the signature algorithm is a Schnorr signature of 160 bits, and that the cryptography used for the presently claimed system is an ElGamal cryptography of 1024 bits, which has a safety equivalent to that of a signature of 160 bits. In such a case, the amount of secret information that must be stored in the system as claimed is 5,120 bits (1024 x 5), as compared to 1,600,000 for the Brickell system (160 x 10,000). Advantageously, in the system as claimed, the amount of secret information that must be stored at the remote host remains constant as the number of mobile agents increases, while in the Brickell system, the amount is proportional to the number.

Independent claims 7, 14 and 18 are likewise patentable over Brickell. Claims 7, 14 and 18 respectively recite "a partial signature calculation means to which signature target data, the signature target data being target data to which a digital signature of the owner is to be attached, data which have been carried by the mobile agent including the partial signature auxiliary data, and a secret key of the remote host are inputted and which calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent", "a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, the signature target data being target data to which a digital signature of the owner of the mobile agent is to be attached, data which have been carried by the mobile agent including partial signature auxiliary data which has been generated based on generated random numbers and a secret key of the owner at a base host, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of the owner of the mobile agent for the signature target data", and "a partial signature calculation process for receiving signature target data which has been arbitrarily presented to the mobile agent by a remote host, the signature target data being target data to which a digital signature of the owner of the mobile agent is to be attached, data which have been carried by the mobile agent

including partial signature auxiliary data which has been generated based on generated random numbers and a secret key of the owner at a base host, and a secret key of the remote host as input data, and calculating a partial signature which is necessary for the calculation of a digital signature of the owner of the mobile agent for the signature target data." Thus, claims 7, 14 and 18 are patentable for reasons analogous to those above with respect to claim 1.

Claims 13 and 17 respectively recite "generating partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts" and "generating partial signature auxiliary data for distributing the information of the newly generated secret key to remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of a digital signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for the partial signature auxiliary data using a secret key of the owner of a mobile agent." These features are not disclosed in Brickell, and thus claims 13 and 17 are patentable thereover.

The dependent claims depend from one of the respective independent claims, and are patentable for at least the same reasons, as well as for further patentable features recited therein.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of

papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date January 4, 2006 By _____

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Thomas G. Bilodeau
Attorney for Applicant
Registration No. 43,438